Attorney Docket No **NG(MS)7194** **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s)	Kenneth Aull, et al.	Confirmation No.:	2941
Application No.:	10/027,622	Examiner:	Nadia Khoshnoodi
Filing Date:	December 19, 2001	Group Art Unit:	2137
Title:	**ASSIGNMENT OF USER CERTIFICATES/PRIVATE KEYS IN TOKEN ENABLED PUBLIC KEY INFRASTRUCTURE SYSTEM**		

Mail Stop AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER FOR RESPONSE/AMENDMENT

Transmitted herewith is/are the following in the above-identified application.

☒ **Reply Brief**

☐ Other: _____

CERTIFICATION UNDER 37 CFR §§ 1.8(a) and 1.10*
Express Mail certification is optional.)

FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being transmitted via facsimile to the Patent and Trademark Office at (571) 273-8300

Date of Deposit **August 28, 2007**

Typed Name: **Lisa D. Jones** Pages **13**

Signature: Lisa D. Jones

*Only the date of filing (§ 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under § 1.8 continues to be taken into account in determining timeliness. See § 1.703(f). Consider "Express Mail Post Office Addressee" (§ 1.10) or facsimile transmission (§ 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

CLAIMS AS AMENDED									
(1)	(2)		(3)	(4)	SMALL ENTITY		(5)	LARGE ENTITY	(6)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	FEE	RATE	FEE	ADDITIONAL FEES
TOTAL CLAIMS		MINUS			X $ 25.00		X $ 50.00		
INDEP. CLAIMS		MINUS			X $100.00		X $200.00		
[ ] First Presentation of a Multiple Dependent Claim					$180.00		$360.00		
SUBTOTAL OF ADDITIONAL FEES									

* If the entry in Column 1 is less than entry in Column 2, write "0" in Column 3.
** If the "Highest No. Previously Paid For *in this space* is less than 20, enter "20".
*** If the "Highest No. Previously Paid For" *in this space* is less than 3, enter "3".
The "Highest No. Previously Paid For" *(Total / Independent)* is the highest number found in Col. 1 of a prior amendment / the number of claims originally filed.
WARNING "After final rejection or action (§1.113) amendments may be made canceling claims or complying with any requirement of form which has been made." 37 C.F.R. § 1.116(a)(emphasis added).

Applicant petitions for an extension of time under 37 C.F.R. §1.136
(FEES: 37 C.F.R. §1.17 (1) – (4) for the total number of months checked below:

EXTENSION	1ST MONTH	2ND MONTH	3RD MONTH	4TH MONTH	
Large Entity	☐ $120.00	☐ $450.00	☐ $1,020.00	☐ $1,590.00	
Small Entity	☐ 60.00	☐ 225.00	☐ 510.00	☐ 795.00	$0.00

[ ] *An extension for _____ month(s) has already been secured and the fee paid therefore of $_____ is deducted from the total fee due for the total month(s) of extension now requested.*

[XX] *Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition for extension of time.*

TOTAL ADDITIONAL FEE FOR THIS AMENDMENT	$0.00

FEE PAYMENT

☐ Attached is a ☐ check ☐ money order in the amount of $0.00

☒ Authorization is hereby made to charge the amount of $0.00

☒ to Deposit Account No. 20-0090.

☐ to Credit card as shown on the attached credit card information authorization form PTO-2038.

WARNING: *Credit card information should not be included on this form as it may become public.*

☒ Charge any additional fees required by this paper or credit any overpayment in the manner authorized above.

A duplicate of this paper is attached.

FEE DEFICIENCY

☒ If any additional extension and/or fee is required, charge Deposit Account No. 20-0090.

AND/OR

☒ If any additional fee for claims is required, charge Deposit Account No. 20-0090.

Date: 8/28/07

Signature Of Attorney

Customer No.: 26,294

Reg. No.: 43,660

CHRISTOPHER HARRIS
TAROLLI, SUNDHEIM, COVELL & TUMMINO L.L.P.
1300 East Ninth Street – Suite 1700
Cleveland, OH 44114-1400
Tel. No.:(215) 621-2234

CERTIFICATE OF MAILING/TRANSMISSION (37 C.F.R. 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

_____ deposited with the United States Postal Service, with sufficient postage, as first class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

FACSIMILE

X transmitted by facsimile to the Patent and Trademark Office.

12 total pages including Transmittal.

Signature

Lisa Jones

(type or print name of person certifying)

Date: 28 August 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Kenneth Aull, et al.
Serial No.	:	10/027,622
Filing Date	:	December 19, 2001
For	:	ASSIGNMENT OF USER CERTIFICATES/PRIVATE KEYS IN TOKEN ENABLED PUBLIC KEY INFRASTRUCTURE SYSTEM
Group Art Unit	:	2137
Examiner	:	Nadia Khoshnoodi
Attorney Docket No.	:	NG(MS)7194

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Sir:

This Reply Brief is in response to the Examiner's Answer dated June 29, 2007. This Reply Brief addresses the Examiner's Answer concerning the appealed claims 1-16.

I. **Appealed Claims 1 and 9**

In the Appeal Brief filed March 5, 2007 ("Appeal Brief"), Applicant's representative argued that the claimed element "accessing a token through a token reader connected to a computer system by a certificate authority," as recited in claims 1 and 9, is not taught or suggested by U.S. Patent No. 6,194,131 to Geer, et al. ("Geer") in view of the U.S. Patent No. 6,615,171 to Kanevsky, et al. ("Kanevsky"). The Examiner responded to Applicant's representative's arguments in the Examiner's Answer dated June 29, 2007 ("Examiner's Answer"), by stating the following:

> Geer et al. teaches that information within a token is accessed via a network by a certifying authority in col. 2, lines 27-39 and Figure 1, elements 10, 12 and 18: "a system for implementing a transaction in accordance with the present invention includes an authorizing computer 10, a smart card 12 at authorizing computer 10 that corresponds to a specific user of the authorizing computer 10, an authorized computer 14 that is authorized by authorizing computer 10 to perform some specific action, and a transaction computer 16 that performs a transaction with authorized computer 14 that includes the authorized computer 14 performing the authorized action. The system also includes a certifying authority 18 that performs the conventional function of certifying the identity of the user to authorized computer 14 and transaction computer 16." In the previously cited portion, Geer teaches that a certifying authority is necessary to certify the identity of the user to the authorized computer and to the transaction computer. Thus, in order to perform the operations of the invention disclosed by Geer, the certificate authority must have access to the user's information via the smart card, i.e. the token in order to be able to prove the user's true identity to the computers that the user is requesting some type of service from (Examiner's Answer, Page 8).

Applicant's representative respectfully disagrees with the Examiner's conclusion that the certifying authority 18 disclosed in Geer, must have access to the user's information via the smart card 12 to prove

the identity of the user. For instance, in Geer the authorizing computer 10 could communicate with the smart card 12, and then send information to the certifying authority 18 requesting that proof of the user's identity be sent to the computers to which the user is requesting service. Such an implementation of Geer would not require any access (or even any communication) to exist between the smart card 12 and the certifying authority 18.

Applicant's representative respectfully submits the Examiner's conclusion (that the certifying authority 18 must be able to access the smart card 12) is based not on the teachings and suggestions of the cited art, but rather on the present application. To imbue one of ordinary skill in the art with knowledge of the invention under consideration, when no prior art reference or references of record convey or suggest that knowledge, is to fall victim to the insidious effect of a hindsight syndrome, wherein the teachings of the invention are used against itself. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 U.S.P.Q. 303, 312-313 (Fed. Cir. 1983). Accordingly, Applicant's representative respectfully submits that the Examiner is incorrect in her analysis of the cited art, and thus has failed to show that the element of "accessing a token through a token reader connected to a computer system by a certificate authority," as recited in claims 1 and 9, is taught or suggested by the cited art.

In the Appeal Brief, Applicant's representative argued that the element "downloading a certificate and an associated private key to a

token," as recited in claims 1 and 9, is not taught or suggested by Geer taken in view of Kanevsky, when claims 1 and 9 are read as a whole. In response, the Examiner stated the following:

> "Referring to FIG. 6, in operation of the system of FIG. 5, each of the actual parties to the business obtains, from a certifying authority computer operated by an investment banking firm, an authorizing certificate and a private key of a new public key pair minted by the certifying authority computer (step 78)." Furthermore, since Geer also discloses that the invention uses smart cards, each of the parties in the embodiment where a business deal is conducted are presumed to use a smart card for maintaining the certificate and private key sent... (See Examiner's Answer, Page 9).

Applicant's representative respectfully submits that the Examiner is once again failing to read claims 1 and 9 as a whole. The determination of obviousness requires an evaluation of the claimed invention *as a whole*, and not merely the difference between the claimed invention and the prior art. *Lear Siegler, Inc. v. Aeroquip Corp.*, 733 F.2d 881, 221 U.S.P.Q. 1025, 1033 (Fed. Cir. 1984). In claims 1 and 9, the token to which the certificate and associated private key are downloaded, is the same token from which a certificate is read. In analyzing claims 1 and 9, it is respectfully submitted the Examiner has failed to cite any section of Geer that teaches or suggests that the authorization certificate and a private key minted by the certifying authority computer are downloaded to a smart card (e.g., token) from which a user signature certificate is read, as would be required if the authorization certificate and the private key disclosed in Geer were to read on the certificate and associated private key recited in claims 1 and 9. Accordingly, Applicant's representative respectfully submits that the Examiner has failed to consider claims 1 and 9 as a whole, and thus has failed to show that the element of

"downloading a certificate and an associated private key to a token," as recited in claims 1 and 9 is taught or suggested by the cited art, when claims 1 and 9 are read as a whole.

In the Appeal Brief, Applicant's representative argued that the element "searching for a match for the token ID and the user signature certificate in an authoritative database, and that a certificate and an associated private key are wrapped with a public key associated with the token ID if a match is found for the token ID and the user signature certificate is found in the authoritative database," as recited in claims 1 and 9 is not taught or suggested by Geer taken in view of Kanevsky. In response, the Examiner stated the following:

> [a]lthough Kanevsky suggests returning a new PIN to the user, when modifying Geer, the new PIN is replaced with the new conversation certificate along with its associated private key. One would have been motivated to modify the method disclosed in Geer et al. with Kanevsky because doing so not only ensures that the information transmitted is both confidential and can only be decrypted by the user who has a the private key associated with the public key of the smartcard, but allows for stronger means of authenticating each business partner before allowing that entity access to highly confidential information.

Applicant's representative respectfully submits that the reason for combining and modifying the teachings of Geer and Kanevsky provided by the Examiner appears to be based on improper hindsight. Applicant's representative respectfully submits that the cited art (e.g., Geer and Kanevsky) has security holes that the present application overcomes. In particular, in the methodology and computer program recited in claims 1 and 9 respectively, the user signature certificate is wrapped with a public key associated with a token ID. Thus, the user signature

certificate is encrypted and cannot be decrypted without using a private key stored on the token (the decryption step is also recited in claims 1 and 9). The methodology and computer program recited in claims 1 and 9 respectively can prevent unauthorized access of the signature certificate by malicious programs that may intercept the encrypted certificates (e.g., "Trojan Horses", See Spec., Pars. [0010] and [0013]). Neither Kanevsky nor Geer even considers the possibility that such malicious programs can pose a security threat. Accordingly, Applicant's representative respectfully submits that the Examiner has failed to show that "searching for a match for the token ID and the user signature certificate in an authoritative database, and that a certificate and an associated private key are wrapped with a public key associated with the token ID if a match is found for the token ID and the user signature certificate is found in the authoritative database," as recited in claims 1 and 9, is taught or suggested by the cited art.

In the Appeal Brief, Applicant's representative argued that there is no motivation to combine and modify the teachings of Geer and Kanevsky in the manner suggested by the Examiner since the purported combination would require a tradeoff of convenience for increased security and complexity, which would be contrary to current patent case law. The Examiner's response included the following:

> Thus, the combination of Geer and Kanevsky result in a system which is more likely to prevent unauthorized users to gain access to confidential information. Furthermore, in response to Appellant's statement that "Geer does not even mention the employment of token IDs," Examiner would like to note that the term token ID is not specifically defined, thus, for all purposes a token ID may even be interpreted (according to MPEP 2111) as the public/private key pair which is unique to each smart card disclosed... (See Examiner's Answer Page 14).

Applicant's representative respectfully submits that the Examiner failed to address Applicant's representative's argument that combining and modifying the teachings of Geer and Kanevsky would result in a less convenient system, but instead argues that the motivation to combine and modify Geer and Kanevsky arises solely from an increase in security. Thus, Applicant's representative respectfully submits that the Examiner has failed to establish a proper motivation to combine and modify the teachings of Geer and Kanevsky.

Furthermore, in response to the Examiner's argument that a public/private key pair can read on a token ID, Applicant's representative respectfully disagrees. Claims 1 and 9 recite a token ID, a public key associated with the token ID, and a private key. Applicant's representative respectfully submits that any interpretation of claims 1 and 9 that would have a public/private key pair being equivalent to a token ID would be an interpretation contrary to a normal claim interpretation. A claim construction that gives meaning to all the terms of the claim is preferred over one that does not do so. *Merck & Co. v. Teva Pharms. USA, Inc.*, 395 F.3d 1364, 1372, 73 U.S.P.Q.2D 1641 (Fed. Cir. 2005). Thus, Applicant's representative respectfully submits that the Examiner is attempting to construe claims 1 and 9 such that not all of the terms recited (e.g., token ID) are given meaning, since the Examiner contends that the token ID is equivalent to other terms recited in claims 1 and 9 (e.g., public and private keys). Accordingly, Applicant's representative respectfully submits that the Examiner has failed to establish a proper motivation for combining and modifying the teachings of Geer and Kanevsky in the manner suggested by the Examiner. Thus, for the reasons stated above, Applicant's representative maintains that claims 1 and 9 are patentable over Geer taken in view of Kanevsky.

II. **Appealed Claims 2 and 10**

In the Appeal Brief, Applicant's representative argued that the element "a certificate and associated private key is a plurality of certificates and associated private keys, wherein at least one of the certificates and associated private keys is a signature certificate for the user, an encryption certificate and associated private key for the user, and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy," as recited in claims 2 and 10, is not taught or suggested by Geer taken in view of Kanevsky, when claims 2 and 10 are read in light of their corresponding independent claims, namely claims 1 and 9, respectively. In response, the Examiner cited various sections of Geer that the Examiner contends discloses different kinds of certificates (See Examiner's Answer, Pages 14-16). Applicant's representative respectfully submits that the Examiner's response failed to address Applicant's representative's point made in the Appeal Brief that since claims 2 and 10 depend from claims 1 and 9, respectively, the plurality of certificates and private keys recited in claims 2 and 10 is downloaded to the token, which is the same token from which a user signature certificate is read. Accordingly, Applicant's representative maintains that claims 2 and 10 are patentable over Geer taken in view of Kanevsky.

III. **Appealed Claims 7 and 15**

In the Appeal Brief, Applicant's representative argues Geer, Kanevsky and U.S. Patent Pub. No. 2003/0005291 to Burn ("Burn") teach away from their combination and modification in the manner suggested by the Examiner since the purported combination would result in an inoperable device. In the Examiner's Answer, Examiner responds by stating:

> [t]he test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). In this case, one would have been motivated to modify the teachings of Geer in view of Kanevsky by Burn in order to incorporate yet another layer of security which is to require that a user enter a password before the operations may be performed as suggested by Burn...

Applicant's representative respectfully submits the Examiner has misconstrued the cited art references. It is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the claimed invention is rendered obvious. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q. 2d 1780 (Fed. Cir. 1992). One cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q. 2d 1596 (Fed. Cir. 1988). Applicant's representative respectfully submits that the Examiner is attempting to use claims 7 and 15 as the aforementioned template, since it appears that the Examiner is attempting to use small parts (modified considerably) of each cited art reference to support her arguments. Accordingly, Applicant's representative

respectfully maintains the position that combining and modifying the teachings of Geer, Kanevsky and Burn would result in an inoperable device, and thus, claims 7 and 15 are patentable over the cited art.

CONCLUSION

In view of the foregoing remarks, Applicant's representative respectfully submits that the present application is in condition for allowance. Applicant's representative respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 28 August 2007

Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
1300 EAST NINTH STREET, SUITE 1700
CLEVELAND, OHIO 44114
Phone: (216) 621-2234
Fax: (216) 621-4072

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.